Beschreibung

Redundantes Automatisierungssystem zur Steuerung einer technischen Einrichtung sowie Verfahren zum Betrieb eines derartigen Automatisierungssystems

Die Erfindung betrifft ein redundantes Automatisierungssystem zur Steuerung einer technischen Einrichtung sowie ein Verfahren zum Betrieb eines solchen Automatisierungssystems, wobei mindestens zwei Automatisierungsgeräte vorhanden sind. Ein erstes dieser Automatisierungsgeräte wird dabei als Master-Automatisierungsgerät und ein zweites der Automatisierungsgeräte als Stand-by-Automatisierungsgerät betrieben.

Die permanente Verfügbarkeit von Geräten und Systemen ist bei der Automatisierung einer technischen Anlage - insbesondere einer Kraftwerksanlage - eine der wichtigsten Anforderungen. Aus Gründen der Sicherheit zum Ausschluss einer möglichen Gefährdung sowie aus Gründen einer sicheren Versorgung mit elektrischer Energie oder Gütern muss der Ausfall von Automatisierungssystemen und ein damit verbundener Stillstand von wichtigen technischen Anlagen weitestgehend vermieden werden.

Zur Lösung dieses Problems sind im Stand der Technik sogenannte hochverfügbare Automatisierungssysteme, beispielsweise SIMATIC S-7 H der Firma Siemens, bekannt, bei welchen praktisch alle Komponenten inkl. der Speicher- und Stromversorgungseinheiten redundant vorhanden sind, so dass im Falle eines Fehlers eines Automatisierungsgerät auf ein anderes, identisch aufgebautes Automatisierungsgerät unterbrechnungsfrei umgeschaltet werden kann. Die Automatisierungsgeräte sind dabei hinsichtlich ihrer Befehlsausführung zueinander synchronisiert, so dass in beiden Automatisierungsgeräten vollkommen zeitparallel dieselben Daten verarbeitet werden und die selben Befehle ausgeführt werden. So ist es möglich, dass ein derartig betriebenes Stand-by-Automatisierungsgerät

die Funktion eines fehlerbehafteten Master-Automatisierungsgeräts übernimmt.

Derartige hochverfügbare Automatisierungssysteme sind bisher praktisch ausschließlich auf Basis sogenannter speicherprogrammierbarer Steuerungen (SPS) erhältlich, in ihrer Anwendung kompliziert und in ihrer Anschaffung sehr kostspielig.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Automatisierungssystem der eingangs genannten Art anzugeben, welches einfacher aufgebaut ist und bei welchem insbesondere Standardkomponenten aus der Personal Computer-Technik weitestgehend eingesetzt werden können.

Bezüglich des Automatisierungssystems wird die Aufgabe gelöst durch ein redundantes Automatisierungssystem zur Steuerung einer technischen Einrichtung mit den Merkmalen des unabhängigen Patenanspruchs 1.

Die Erfindung geht dabei von der Überlegung aus, dass eine der wichtigsten Vorraussetzungen zur Realisierung eines redundanten Automatisierungssystems in der Bereitstellung einer aktuellen Datenbasis, welche den Zustand der technischen Einrichtung und des Automatisierungssystems beschreibt, zu sehen ist. Eine Umschaltung von dem Master-Automatisierungsgerät auf das Stand-by-Automatisierungsgerät ohne merkliche Verzögerung ist dabei nur dann erreichbar, wenn beiden Automatisierungsgeräten zum Zeitpunkt des Auftretens eines Fehlers die gleichen aktuellen Daten zur Verfügung stehen, so dass ein Umschalten auf das Reservegerät sofort und ohne „Datensprünge" möglich ist.

Im Stand der Technik der hoch verfügbaren speicherprogrammierbaren Steuerungen wird dies dadurch gelöst, dass beide Automatisierungsgeräte identisch aufgebaut sind und u.a. jeweils eine Speichereinheit umfassen, in welche aufgrund der oben bereits beschriebenen befehlssynchronen Abarbeitung die

gleichen Daten geschrieben und die gleichen Daten ausgelesen werden.

Im Unterschied dazu ist bei der vorliegenden Erfindung vorgesehen, dass zwar zwei Automatisierungsgeräte vorhanden sind, dass aber für diese nur eine gemeinsame Speichereinheit vorgesehen ist, auf welche beide Automatisierungsgeräte Schreib- und Lesezugriff haben. Insofern ist zum Stand der Technik der Realisierungsaufwand erheblich reduziert, da zum einen nur eine Speichereinheit notwendig ist und zum anderen daraus folgendend der erforderliche Synchronisationsaufwand zwischen mehreren Speichereinheiten der Automatisierungsgeräte entfällt.

Die weitaus meisten Ausfälle von Automatisierungsgeräten gehen auf Fehlfunktionen beispielsweise der Ein- oder Ausgabekarten, der Stromversorgung oder der CPUs der Automatisierungsgeräte zurück; von daher gesehen bietet die vorliegende Erfindung eine wirtschaftliche, vereinfachte Lösung für die meisten in der Praxis zu bewältigenden Redundanzprobleme der Automatisierung.

Obwohl bereits einige Automatisierungslösungen auf PC-Basis existieren, können diese bislang noch nicht ein stoßfreies Umschalten auf das Reserve-Automatisierungsgerät gewährleisten, da die erforderliche Synchronisation der Datenbasen, auf welche die Automatisierungsgeräte zugreifen, mit bekannten Mitteln nicht in der erforderlichen Geschwindigkeit stattfinden kann. Ein stoßfreies Umschalten bedeutet dabei, dass das Umschalten vom Master- auf das Reserve-Automatisierungsgerät (Stand-by-Automatisierungsgerät) praktisch ohne Auswirkungen auf die Ein- und Ausgangssignale des Automatisierungssystem. geschieht, so dass insbesondere Regelungen an genau der Stelle weiter geführt werden, an welcher das fehlerbehaftete Automatisierungsgerät die Regelung abgebrochen hat. Dem Reserve-Automatisierungssystem müssen folglich zum Zeitpunkt der Übernahme der Regelung sogenannte Anfangswerte zur Verfügung

stehen, welche die Vergangenheit des Regelungsvorgangs betreffen (umfasst sind dabei insbesondere Regelungsalgorithmen, welche einen Integral- und/oder Differenzialanteil aufweisen).

Die vorliegende Erfindung löst das Problem einer aktuellen Datenbasis für die Automatisierungsgeräte dahingehend, dass dafür nur eine gemeinsame Speichereinheit vorgesehen ist.

Eine Lösung zur Realisierung einer derartigen Speichereinheit in PC-Technik bei einem erfindungsgemäßen Automatisierungssystem umfasst beispielsweise den Einsatz sogenannter „Reflective Memories", welche als kommerziell erhältliche PC-Baugruppen zur Verfügung stehen.

Dadurch werden PCs, Workstations oder „Embedded-Systems" (insbesondere mit unterschiedlichen Betriebssystemen), in die Lage versetzt, praktisch in Echtzeit auf eine gemeinsame Datenbasis zuzugreifen.

Bei einem lokalen Rechner befindet sich die Reflective Memory-Baugruppe beispielsweise im Adressraum des gemeinsamen Speichers der beteiligten Rechner eines Netzwerks. Dann können Daten von jeder Automatisierungsebene aus, insbesondere auch von einer Anwendersoftware, direkt in diesen Speicherbereich geschrieben und aus diesem Speicherbereich ausgelesen werden. Daten, die der lokale Rechner in diesen „Reflective Memory" schreibt, stehen dann automatisch allen anderen Rechnern parallel und ohne Zeitverzögerung zur Verfügung.

Aufgrund der besonderen technischen Ausbildung der Reflective Memory-Baugruppe beeinflusst der dabei stattfindende Datentransport zwischen den Rechnern die normale Performance dieses Rechners nicht.

In einer vorteilhaften Ausgestaltung der Erfindung ist weiterhin ein Überwachungsmodul vorgesehen, mittels welchem der

Betrieb des Master-Automatisierungssystems überwachbar und im Falle eines Fehlers des Master-Automatisierungsgeräts ein Umschalten auf das Stand-by-Automatisierungsgerät ermöglicht ist, welches daraufhin die Funktion des bisherigen Master-Automatisierungsgeräts übernimmt.

Bei dieser Ausführungsform ist eine Überwachung der Gerätefunktion inklusive einer Fehlererkennung realisiert. Beispielsweise umfasst das Überwachungsmodul dabei die Auswertung eines sogenannten Lebenszeichens des Master-Automatisierungsgeräts, wobei z.B. bei jedem Zyklus der Überprüfung ein Kennwert verändert wird, falls das Master-Automatisierungsgerät funktionstüchtig ist. Sollte dieser Kennwert bei einem Zyklus nicht verändert werden, so ist dies ein Indiz für einen Fehler dieses Automatisierungsgeräts und das Überwachungsmodul nimmt den Umschaltvorgang auf das zugeordnete Stand-by-Automatisierungsgerät vor.

Mögliche Fehler, welche eine Veränderung des genannten Kennwerts verhindern, umfassen beispielsweise Hardware-Fehler und/oder Betriebssystem-Fehler und/oder Anwendersoftwarefehler.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung sind im gemeinsamen Speicherbereich solche Zustandsdaten vorhanden, welche den aktuellen Betriebszustand der technischen Einrichtung und des Automatisierungssystems unmittelbar vor dem Zeitpunkt des Auftretens eines Fehlers des Master-Automatisierungsgeräts beschreiben.

Dadurch ist es möglich, dass das Stand-by-Automatisierungsgerät die Funktion des bisherigen Master-Automatisierungsgeräts sofort übernehmen kann, da alle dafür notwendigen Daten im gemeinsamen Speicherbereich abgelegt sind und vom Stand-by-Automatisierungsgerät zur Weiterverarbeitung ohne Zeitverzögerung ausgelesen werden können.

Die Zustandsdaten sollen dabei insbesondere solche Daten umfassen, welche Anfangswerten von Regelungsalgorithmen entsprechen, so dass dem Stand-by-Automatisierungsgerät mittels dieser Anfangswerte auch die Historie der betreffenden Regelungsvorgänge bekannt ist und die betreffenden Regelungen vom Stand-by-Automatisierungsgerät kontinuierlich weiter geführt werden können.

Ferner umfassen die Zustandsdaten solche Ein- und Ausgangsdaten der technischen Einrichtung, welche vom Automatisierungssystem erfasst und/oder an die technische Einrichtung abgegeben werden. Die Gesamtheit dieser Daten wird als Prozessabbild bezeichnet.

Besonders vorteilhaft geschieht das Umschalten stoßfrei, indem mindestens ein Teil der im gemeinsamen Speicherbereich vorhandenen Daten vom Stand-by-Automatisierungsgerät als aktuelles Zustandsabbild der technischen Einrichtung und des Automatisierungssystems unmittelbar weiterverarbeitet wird.

Hierbei geschieht das Umschalten zwischen dem Master-Automatisierungsgerät und dem Stand-by-Automatisierungsgerät praktisch ohne Verzögerung unter kontinuierlicher Weiterführung der Steuerung der technischen Einrichtung durch das Stand-by-Automatisierungsgerät.

Die Erfindung führt weiterhin zu einem Verfahren zum Betrieb eines redundanten Automatisierungssystems zur Steuerung einer technischen Einrichtung mit den Merkmalen des unabhängigen Patentanspruchs 5.

Vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens sind in den zugehörigen abhängigen Patentansprüchen niedergelegt.

Im Folgenden wird ein Ausführungsbeispiel der Erfindung näher dargestellt.

Es zeigt:

FIG ein erfindungsgemäßes redundantes Automatisierungssystem.

In der Figur ist ein erfindungsgemäßes redundantes Automatisierungssystem 1 dargestellt, welches Automatisierungsgeräte 3a,3b umfasst. Ein erstes Automatisierungsgerät ist dabei ausgebildet als ein Master-Automatisierungsgerät 3a, welches die Steuerung einer technischen Einrichtung übernimmt. Die Signale aus der technischen Einrichtung sowie die Steuerbefehle an die technische Einrichtung werden dabei von Feldgeräten 17 verarbeitet und über einen Feldbus 15 an die Automatisierungsgeräte 3a,3b übermittelt.

Im Falle eines Fehlers des ersten Automatisierungsgeräts 3a steht ein zweite Automatisierungsgerät zur Verfügung, welches als Stand-by-Automatisierungsgerät 3b ausgebildet ist und die Steuerungsaufgaben des ersten Automatisierungsgeräts 3a übernehmen kann.

Zur Fehlererkennung und Umschaltung vom ersten Automatisierungsgerät 3a auf das zweite Automatisierungsgerät 3b ist ein Überwachungsmodul 23 vorgesehen. Dieses wertet u.a. ein Lebenszeichen 25 des ersten Automatisierungsgeräts 3a aus und schaltet im Fehlerfall auf das zweite Automatisierungsgerät 3b um, welches daraufhin die Steuerungsaufgaben des bisherigen Master-Automatisierungsgeräts 3a übernimmt.

Die Automatisierungsgeräte 3a,3b besitzen jeweils eine CPU 5a,5b und ggf. einen Speicher 6a,6b. Sie sind bevorzugt ausgebildet als Personal Computer, bei welchen die Steuerungsaufgaben als Tasks 7a,7b aufgerufen und ausgeführt werden. Im Vergleich zu herkömmlichen speicherprogrammierbaren Steuerungen laufen diese Automatisierungs-Tasks 7a,7b deutlich schneller ab, weshalb bei derartig ausgebildeten Automatisierungsgeräten auf PC-Basis keine Befehlssynchronisation, son-

dern eine Task-Synchronisation stattfindet. Die Synchronisation der sich jeweils entsprechenden Tasks 7a,7b findet mittels Interrupts 11 statt.

Im Normalbetrieb, wenn das erste Automatisierungsgerät fehlerfrei als Master-Automatisierungsgerät 3a funktioniert, werden die Daten aus der technischen Einrichtung, welche durch die Feldgeräte 17 erfasst sind, von beiden Automatisierungsgeräten 3a,3b mittels jeweils mindestens eines Lesevorgangs 19 laufend eingelesen; die Ausgabe von Steuerungsbefehlen und sonstigen Einwirkungen auf Komponenten der technischen Einrichtung findet jedoch nur durch das Master-Automatisierungsgerät 3a mittels mindestens eines Schreibvorgangs 21 statt.

Nach einem Umschalten auf das bisherige Stand-by-Automatisierungsgerät im Fehlerfall wird dieser Schreibvorgang 21 vom zweiten Automatisierungsgerät 3b übernommen; dies ist in der Figur durch eine gestrichelte Verbindung vom zweiten Automatisierungsgerät 3b zum Feldbus 15 angedeutet.

Bei der Synchronisation der Automatisierungs-Tasks 7a,7b mittels der Interrupts 11 findet vor jedem Task-Aufruf eine Synchronisation von Timern, Zählern, Prozessdaten und ggf. weiterer interner sowie externer Daten statt.

Erfindungsgemäß ist beiden Automatisierungsgeräten 3a,3b eine Speichereinheit 9 zugeordnet, auf welche beide Automatisierungsgeräte 3a,3b Zugriff haben. In dieser Speichereinheit sind im Wesentlichen Zustandsdaten der Automatisierungsgeräte 3a,3b gespeichert, wobei die Speichereinheit 9 mindestens einen Speicherbereich umfasst, der von beiden Automatisierungsgeräten 3a,3b beschreib- und lesbar ist. Auf diese Weise sind zumindest die in diesem Speicherbereich vorhandenen Daten den Automatisierungsgeräten 3a,3b parallel zur Verfügung gestellt. Da die beiden Automatisierungsgeräte 3a,3b somit über eine gemeinsame Datenbasis in Form der Speichereinheit 9 ver-

fügen, auf welche sie jeweils Zugriff haben, muss im Falle eines Fehlers des Master-Automatisierungsgeräts 3a kein Speicherabgleich zwischen den Automatisierungsgeräten 3a und 3b erfolgen, zumindest was den Abgleich der oben genannten Zustandsdaten angeht. Deshalb kann im Fehlerfall eine Umschaltung vom Master-Automatisierungsgerät 3a auf das Stand-by-Automatisierungsgerät 3b sehr schnell und stoßfrei erfolgen, wobei im Vergleich zu bekannten redundanten Automatisierungssystemen der Realisierungsaufwand reduziert ist. Die im gemeinsamen Speicherbereich der Speichereinheit 9 abgelegten Zustandsdaten der Automatisierungsgeräte 3a,3b umfassen alle Daten, welche einen aktuellen Betriebszustand der Automatisierungsgeräte 3a,3b beschreiben wie beispielsweise die aktuellen Werte der aus der technischen Einrichtung an die Automatisierungsgeräte übermittelten Signale (Prozessabbild), die aktuellen Werte der vom Master-Automatisierungsgerät an die technische Einrichtung übermittelten Signale und Befehle sowie erforderlichenfalls aktuelle Anfangswerte von Regelungsalgorithmen, welche mindestens ein differenzierendes und/oder integrierendes Regelungsglied umfassen.

Die Kenntnis des aktuellen Anfangswerts ist zum Zeitpunkt des Auftretens eines Fehlers des Master-Automatisierungsgeräts wichtig, damit das bisherige Stand-by-Automatisierungsgerät die betreffenden Regelungen kontinuierlich, insbesondere ohne Sprung einer Regelgröße, weiterführen kann.

Die Speichereinheit 9 ist bevorzugt ausgebildet als eine sogenannte „Reflective Memory"-Baugruppe, welche als Baugruppe zur Verwendung bei Personal Computern erhältlich ist. Physikalisch installiert wird diese Baugruppe bevorzugt in einem der Automatisierungsgeräte 3a,3b, wobei die Daten, die dieses Automatisierungsgerät in die Baugruppe schreibt, dann allen anderen Automatisierungsgeräten ebenfalls zur Verfügung stehen.

Zusammenfassend lässt sich die vorliegende Erfindung folgendermaßen umschreiben:

Bei einem erfindungsgemäßen redundanten Automatisierungssystem (1) sowie einem Verfahren zum Betrieb eines solchen Automatisierungssystems (1) sind zwei Automatisierungsgeräte (3a,3b) vorgesehen, welchen eine gemeinsame Speichereinheit zugeordnet ist, auf welche Zustandsdaten die Automatisierungsgeräte (3a,3b) speicherbar sind. Somit haben die Automatisierungsgeräte (3a,3b) unmittelbaren Zugriff auf eine gemeinsame Datenbasis und ein Speicherabgleich im Falle eines Fehlers entfällt beim Umschalten auf das Stand-by-Automatisierungsgerät (3b).

Patentansprüche

1. Redundantes Automatisierungssystem (1) zur Steuerung einer technischen Einrichtung umfassend mindestens zwei Automatisierungsgeräte (3a,3b), wobei ein erstes der Automatisierungsgeräte als Master-Automatisierungsgerät (3a) und ein zweites der Automatisierungsgeräte als Stand-by-Automatisierungsgerät (3b) ausgebildet ist,
g e k e n n z e i c h n e t durch
eine den mindestens zwei Automatisierungsgeräten (3a,3b) zugeordnete Speichereinheit (9), auf welcher Zustandsdaten der Automatisierungsgeräte (3a,3b) speicherbar sind, wobei die Speichereinheit (9) einen gemeinsamen Speicherbereich umfasst, welcher von den mindestens zwei Automatisierungsgeräten (3a,3b) beschreib- und lesbar ist, so dass die in diesem Speicherbereich vorhandenen Daten den Automatisierungsgeräten (3a,3b) parallel zur Verfügung stehen.

2. Redundantes Automatisierungssystem (1) nach Anspruch 1,
g e k e n n z e i c h n e t durch
ein Überwachungsmodul (23), mittels welchem der Betrieb des Master-Automatisierungsgeräts (3a) überwachbar und im Falle eines Fehlers des Master-Automatisierungsgeräts (3a) ein Umschalten auf das Stand-by-Automatisierungsgerät (3b) ermöglicht ist, welches daraufhin die Funktion des bisherigen Master-Automatisierungsgeräts (3a) übernimmt.

3. Redundantes Automatisierungssystem (1) nach Anspruch 1 oder 2,
d a d u r c h g e k e n n z e i c h n e t, dass
im gemeinsamen Speicherbereich solche Zustandsdaten vorhanden sind, welche den aktuellen Betriebszustand der technischen Einrichtung und des Automatisierungssystems (1) unmittelbar vor dem Zeitpunkt des Auftretens eines Fehlers des Master-Automatisierungsgeräts (3a) beschreiben.

4. Redundantes Automatisierungssystem (1) nach Anspruch 2 oder 3,
d a d u r c h g e k e n n z e i c h n e t, dass
das Umschalten stoßfrei geschieht, indem mindestens ein Teil der im gemeinsamen Speicherbereich vorhandenen Daten vom Stand-by-Automatisierungsgerät (3b) als aktuelles Zustandsabbild der technischen Einrichtung und des Automatisierungssystems (1) unmittelbar weiterverarbeitet wird.

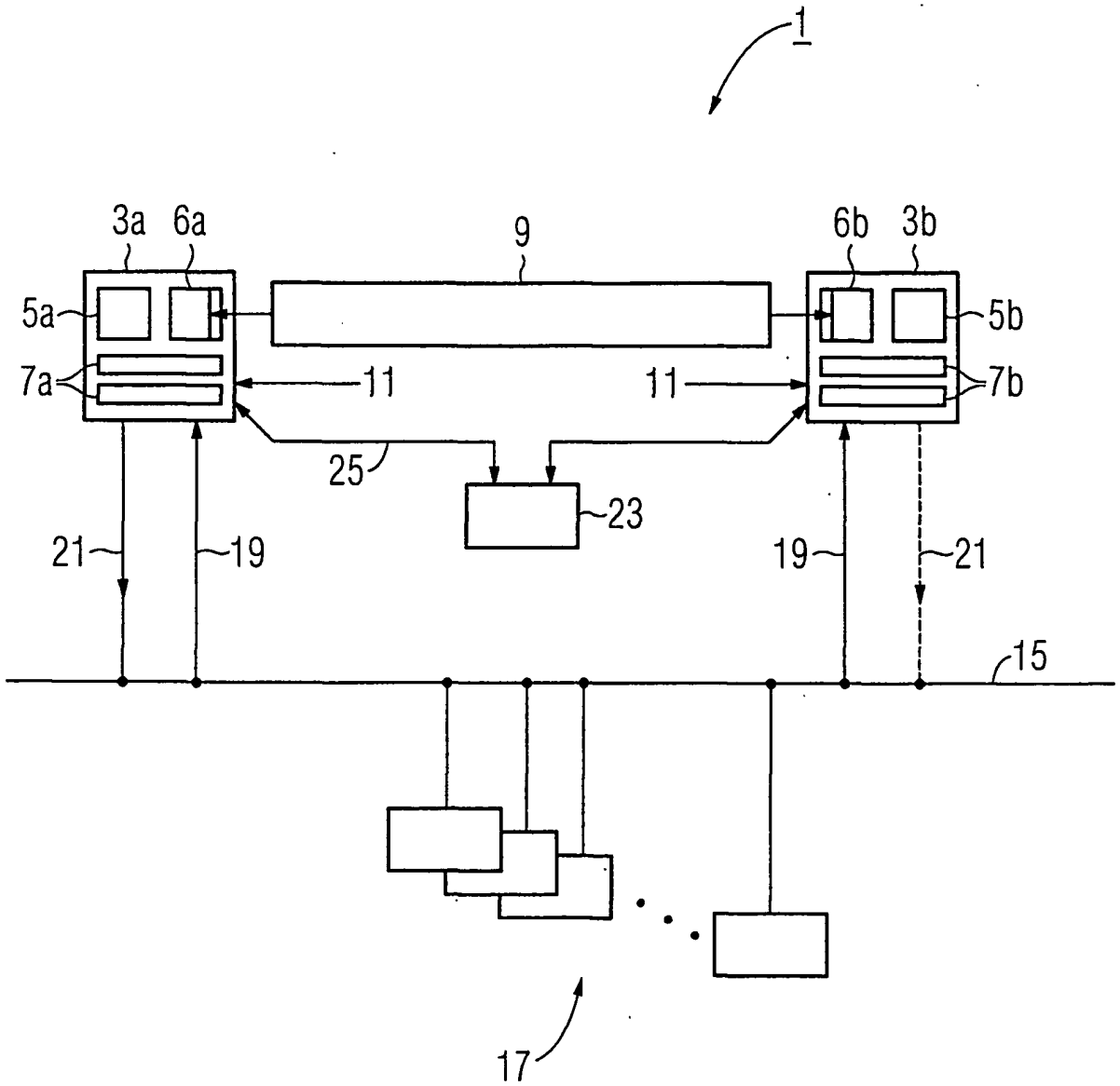
5. Verfahren zum Betrieb eines redundanten Automatisierungssystem (1) zur Steuerung einer technischen Einrichtung umfassend mindestens zwei Automatisierungsgeräte (3a,3b), wobei ein erstes der Automatisierungsgeräte als Master-Automatisierungsgerät (3a) und ein zweites der Automatisierungsgeräte als Stand-by-Automatisierungsgerät (3b) betrieben wird,
d a d u r c h g e k e n n z e i c h n e t, dass
in eine den mindestens zwei Automatisierungsgeräten (3a,3b) zugeordnete Speichereinheit (9) Zustandsdaten der Automatisierungsgeräte (3a,3b) gespeichert werden, wobei ein gemeinsamer Speicherbereich der Speichereinheit von den mindestens zwei Automatisierungsgeräten (3a,3b) beschrieben und ausgelesen werden kann, so dass die in diesem Speicherbereich vorhandenen Daten den Automatisierungsgeräten (3a,3b) parallel zur Verfügung stehen.

6. Verfahren nach Anspruch 5,
d a d u r c h g e k e n n z e i c h n e t, dass
der Betrieb des Master-Automatisierungsgerätsgeräts (3a) überwacht und im Falle eines Fehlers des Master-Automatisierungsgeräts (3a) auf das Stand-by-Automatisierungsgerät (3b) umgeschaltet wird, welches daraufhin die Funktion des bisherigen Master-Automatisierungsgeräts (3a) übernimmt.

7. Verfahren nach Anspruch 5 oder 6,
d a d u r c h g e k e n n z e i c h n e t, dass

im gemeinsamen Speicherbereich solche Zustandsdaten vorhanden sind, welche den aktuellen Betriebszustand der technischen Einrichtung und des Automatisierungssystems (1) unmittelbar vor dem Zeitpunkt des Auftretens eines Fehlers des Master-Automatisierungsgeräts (3a) beschreiben.

8. Verfahren nach Anspruch 6 oder 7,
d a d u r c h g e k e n n z e i c h n e t, dass
das Umschalten stoßfrei durchgeführt wird, indem mindestens ein Teil der im gemeinsamen Speicherbereich vorhandenen Daten vom Stand-by-Automatisierungsgerät (3b) als aktuelles Zustandsabbild der technischen Einrichtung und des Automatisierungssystems (1) unmittelbar weiterverarbeitet wird.


1
3a
6a
9
6b
3b
5a
5b
7a
11
11
7b
25
23
21
19
19
21
15
17